UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,061	02/20/2002	Kunihiko Miyazaki	16869S-043400US	5417

20350 7590 06/05/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/081,061	**Applicant(s)** MIYAZAKI ET AL.	
	Examiner Andrew L. Nalven	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *21 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED INFORMATION

1. Claims 20-35 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claims 20-35 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 20 provides the limitation "wherein the storage unit stores at least one key *created independently of the user*." The specification discloses the creation of keys, but does not have specific support for the creation of a key independent of the user.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 20-23, 25-26, 28-29, and 33-35 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert et al. (US 4,713,753), hereafter Boebert, in view of McCollum et al. (US 6,006,228), hereafter McCollum and Matyas Jr et al (US 6,947,556, hereafter Matyas.

Regarding claim 20, Boebert discloses a computer system having an input/output processing unit for executing a file access, an access execution unit for requesting file access to the input/output processing unit in response to a user instruction, and an access control unit for performing access control when the file access is executed, wherein:

said access control unit (part of secure computer 33 and memory 22) comprises:

a storage unit protected from the access execution unit (memory 22 protected by memory address apparatus 336 in secure processor 33 via access rights 622; col. 10, lines 62-67);

a file list stored on said storage unit describing security levels of files (data objects characteristics table 333; col. 9, lines 65-67);

an access control processing unit for judging whether the file access is legal in accordance with said file list, said user list, an access type (access mode) of file access, information identifying a file, and information identifying a user (secure computer 33; Fig. 3 and 8; col. 7, line 52 – col. 8, line 7; col. 9, lines 21-26; col. 10, lines 28-39); and

an access monitor unit (user entity identification apparatus 31, program working set table 334 and tag code recognition apparatus 336a) which:

sends, when the input/output processing unit executes access, the access type (access mode), the information identifying the file, the information identifying the user to said access control processing unit (apparatus 31 sends user information to current security content register 331 as well as sends file identification and access mode to ordinary data object processing unit 32; col. 7, lines 56-62);

receives a validity judgment (access right 622) as a result of the file access from said access control processing unit (program working set table 334 receives access right 622 from security policy unit 332 via distinguished data object processing unit 335; col. 10, lines 3-5 and 28-67; col. 11, lines 3-11); and

if the file access is legal, makes the input/output processing unit execute the file access, whereas the file access is illegal, inhibits the file access (memory address apparatus 336 executes the file access only where legally permitted by access right 622; col. 9, lines 21-26).

But Boebert does not explicitly explain that said access control unit comprises a user list stored on said storage unit describing clearances of users or an enciphering unit for encrypting a file and a deciphering unit for decrypting a file.

However, Boebert teaches a list of authorized users for the purpose of determining a validity judgment (access right 622) for accessing a file (col. 10, lines 34-39) as well as the maintenance of user information describing security clearance levels by the current security context register 331; col. 9, line 67 – col. 10, line 3). One of ordinary skill in the art would recognize that the authorized list would include information describing security clearance levels because authorization is determined by comparing the clearance level of the requested file to that of the requesting user. Further, McCollum teaches system for securing access to files by employing a user list (User Table 100) describing security clearance levels for the purpose of keeping track of users and their security privileges (Fig. 2; col. 2, lines 62-67). Further, Matyas teaches an enciphering unit for encrypting a file when storing the file on a storage medium (Matyas, column 8 lines 25-41) and a deciphering unit for decrypting the encrypted file when retrieving the encrypted file from the storage medium (Matyas, column 2 lines 36-58) wherein the storage unit stores at least one key created independently of the user, which key is used for both encrypting and decrypting (Matyas, column 2 lines 8-12).

Therefore, it would be obvious to one of ordinary skill to modify the system of Boebert with the teaching of McCollum to provide that said access control unit comprises a user list stored on said storage unit describing clearances of users. One would be motivated to do so in order to facilitate security policy monitoring by keeping track of users and their security privileges. Further, it would be obvious to one of ordinary skill to modify the system of Boebert with the teaching of Matyas to provide encryption and decryption of files using user independent keys. One would be motivated to do so in order to allowing the encrypting of a file whereby authorized users other than the owner may access the file (Matyas, column 4 lines 55-65).

Regarding claim 21, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach an exclusive control unit for protecting a storage area of said storage unit to be used by said access control processing unit from the access execution unit (Boebert: secure processor 33 has exclusive control for protection of memory 22; Fig. 2; col. 3, line 62 – col. 4, line 3; col. 8, lines 7-10).

Regarding claim 22, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 21, and Boebert, McCollum, and Matyas further teach a user setting/managing unit for setting and managing said user list (McCollum: security database; col. 2, lines 33-38; col. 3, lines 41-52).

Regarding claim 23, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 22, but Boebert, McCollum, and Matyas do not explicitly explain that said user list setting/managing unit includes an authentication unit for authenticating a security administrator.

However, Boebert, McCollum, and Matyas teach that the secure processor 33 may be accessed, and data therein manipulated, only by a security administrator (Boebert: security officer; col. 8, lines 17-19) and that the user list resides within the domain of the secure processor 33 (Boebert: col. 10, lines 34-35). The Examiner takes official notice that one of ordinary skill in the art would recognize that an authentication unit for authentication of a security administrator is necessary for maintaining secure handling of the user list because access to the user list by persons other than a trusted security administrator exposes the list to tampering, which in turn jeopardizes the security of the files in memory 22. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that said user list setting/managing unit includes an authentication unit for authenticating a security administrator for the motivation of ensuring that only an authorized security administrator can modify the user list.

Regarding claim 25, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach a file list setting/managing unit for setting and managing said file list (distinguished data object processing unit 335; col. 9, lines 65-67).

Regarding claim 26, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 25, but Boebert, McCollum, and Matyas do not explicitly explain that said file list setting/managing unit includes an authentication unit for authenticating a security administrator.

However, Boebert and McCollum teach that the secure processor 33 may be accessed, and data therein manipulated, only by a security administrator (Boebert: security officer; col. 8, lines 17-19) and that the file list (data object characteristics table 333) resides within the domain of the secure processor 33 (Boebert: Fig. 2). The Examiner takes official notice that one of ordinary skill in the art would recognize that an authentication unit for authentication of a security administrator is necessary for maintaining secure handling of the file list because access to the file list by persons other than a trusted security administrator exposes the list to tampering, which in turn jeopardizes the security of the files in memory 22. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that said file list setting/managing unit includes an authentication unit for authenticating a security administrator for the motivation of ensuring that only an authorized security administrator can modify the file list.

Regarding claim 28, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach an enciphering unit for enciphering a file if the file access for requesting to output a file to said storage unit is legal and a deciphering unit for deciphering the enciphered file if the file access for requesting to input the enciphered file from said storage unit is legal (Matyas, column 14 lines 4-12, column 13 lines 27-40).

Regarding claim 29, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 28, but Boebert, McCollum, and Matyas do not explicitly explain an exclusive control unit that protects from the access execution unit a storage area in said storage unit storing at least one key information set to be used by said enciphering unit and said deciphering unit.

However, the Examiner takes official notice that one of ordinary skill would recognize that where the modified system of Boebert, McCollum, and Matyas maintains exclusive control over the encrypted file system in memory 22, the system must also maintain exclusive control over at least one key information set to be used for enciphering and deciphering files in order to ensure the security of the file system, particularly where the cryptographic operations are integrated into the operating system of the secure computer 33. Therefore, it would be obvious to one of ordinary skill in the art to modify the modified system of Boebert, McCollum, and Matyas to provide for an exclusive control unit that protects from the access execution unit a storage area in said storage unit storing at least one key information set to be used by said enciphering unit and said deciphering unit for the motivation of enhancing security.

Regarding claim 33, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach that the access control unit is realized by a software module (col. 8, lines 20-25). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 34, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach that the access control unit is realized by a hardware module (col. 8, lines 19-20; col. 13, lines 51-64). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 35, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, and Boebert, McCollum, and Matyas further teach the key being a symmetric key (Matyas, column 14 lines 35-39). Therefore, for reasons applied above, such a claim also would have been obvious.

4. **Claims 24 and 27 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert, in view of McCollum and Matyas and further in view of Digital Equipment Corporation ("Security," March 1996), hereafter DEC.

Regarding claim 24, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 23, but Boebert, McCollum, and Matyas do not explicitly explain that security administrator is different from a system administrator who manages the access execution unit.

However, Boebert, McCollum, and Matyas teach that the administrator is a security officer (Boebert: col. 8, lines 17-19). And DEC teaches a computer system wherein a securityadministrator is different from a system administrator, who manages the access execution unit, for the purpose of enhancing security by providing checks and balances via the separation of security-related tasks from other administrative tasks (pages 12-14, particularly sections 6.5.1.1 and 6.5.1.2).

Therefore, it would be obvious to one of ordinary skill to modify the modified system of Boebert and McCollum with the teaching of DEC to provide that the security administrator is different from the system administrator who manages the access execution unit. One would be motivated to do so in order to enhance security by providing checks and balances via the separation of security-related tasks from other administrative tasks, particularly where the file system is protected by a secure computer.

Regarding claim 27, this claim is rejected for the same reasons as provided above for claim 26.

5. **Claim 30 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert, in view of McCollum and Matyas, further in view of Scheidt et al. (US 6,754,820), hereafter Scheidt.

Regarding claim 30, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, but Boebert, McCollum, and Matyas do not explicitly explain that said enciphering unit and said deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list.

However, Scheidt further teaches an access control system wherein an enciphering unit and a deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list for the purpose of providing a more balanced security approach (different keys and different cryptographic algorithms are used for each security level in providing secure access to a user of protected information; col. 4, lines 33-57; col. 5, lines 10-27 and 38-50; col. 6, lines 34-37; col. 7, lines 15-32).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the modified system of Boebert, McCollum, and Matyas with the teaching of Scheidt to provide that said enciphering unit and said deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list. One would be motivated to do so in order to provide a more balanced security approach to multiple-level access control.

6. **Claims 31-32 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert in view of McCollum and Matyas, and further in view of Dryer et al. (US 2002/0099666), hereafter Dryer.

Regarding claim 31, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 20, but Boebert, McCollum, and Matyas do not explain an input/output monitor unit for monitoring that the input/output processing unit or said access monitor unit is not tampered or performs a predetermined operation, and instructing to inhibit an input/output of a file if the input/output processing unit or said access monitor unit is tampered or performs an operation different from the predetermined operation.

However, Dryer teaches a secure file access control system wherein an input/output monitor unit (file access monitor 134 and internal integrity checks 132) for monitoring that the secure computer system (Lockbox, which contains a secure file system) is not tampered, and instructing to inhibit operation of the secure computer if secure computer is tampered for the purpose of protecting the data within the secure computer from tampering and other unauthorized access (detection of tampering triggers alarm; para. 0012 and 0023) for the purpose of enhancing security, particularly where a high degree of confidentiality is required (para. 0011). As Boebert and McCollum teach that the input/output processing unit and the access monitor unit operate within a secure computer, one of ordinary skill would recognize that tampering with the input/output processing unit or the access monitor unit is tampering with the secure computer and its associated file system. Further, as Boebert and McCollum teach that access to files is inhibited where the "modes and manners of access" are not permitted (Boebert: col. 9, lines 23-29), one of ordinary skill in the art would also recognize that where tampering is detected, particularly to the level where it raises an alarm, access to secure files would be inhibited in order to protect the files from any potential unauthorized access until the alarm was resolved.

Therefore, it would be obvious to modify the modified system of Boebert and McCollum with the teaching of Dryer to provide an input/output monitor unit for monitoring that the input/output processing unit or said access monitor unit is not tampered or performs a predetermined operation, and instructing to inhibit an input/output of a file if the input/output processing unit or said access monitor unit is tampered or performs an operation different from the predetermined operation. One would be motivated to do so in order to enhance security, particularly where a high degree of confidentiality is required.

Regarding claim 32, the modified system of Boebert, McCollum, and Matyas is relied upon as applied to claim 1, but Boebert, McCollum, and Matyas do not explain a file

access log processing unit for storing and managing information on each file access sent to said access control processing unit.

However, Dryer teaches a file access log processing unit (logging task 130) for storing and managing information on each file access sent to said access control processing unit (para. 0012) for the purpose of enhancing security (para. 0011).

Therefore, it would be obvious to modify the modified system of Boebert and McCollum with the teaching of Dryer to provide for a file access log processing unit for storing and managing information on each file access sent to said access control processing unit. One would be motivated to do so in order to enhance security.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER